

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*Information associated with the Google accounts
nasermunshid16@gmail.com and
abubadriliraqi@gmail.com that is stored by Google LLC

Case No.

3:18mj653

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 18 USC 2339B

Offense Description
 Providing and Attempting to Provide Material Support and Resources to a Foreign Terrorist Organization

The application is based on these facts:
 See Attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

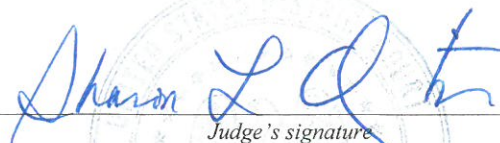

Applicant's signature

P. Andrew Gragan, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 9-21-18City and state: Dayton, Ohio


Judge's signature

Sharon L. Ovington, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, P. Andrew Gragan, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), United States Department of Justice, Cincinnati Division. I have been employed as a Special Agent with the FBI since May 2016. I have received training in national-security investigations and criminal investigations, and I have conducted investigations related to international terrorism, domestic terrorism, white-collar crimes, drug trafficking, public corruption, and violent crimes. As part of these investigations, I have participated in physical surveillance and records analysis, worked with informants, conducted interviews, served court orders and subpoenas, and executed search warrants.

2. I make this affidavit in support of an application for a search warrant for information associated with the account **nasermunshid16@gmail.com** (“SUBJECT ACCOUNT 1”) and **abubadraliraqi@gmail.com** (“SUBJECT ACCOUNT 2”) (collectively the “SUBJECT ACCOUNTS”), as more fully described in Attachment A, which is stored at premises controlled by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

3. Based on my training and experience, and the facts as set forth in this affidavit, I submit there is probable cause to believe that violations of 18 U.S.C. § 2339B (providing and attempting to provide material support and resources to a foreign-terrorist organization) have been committed by **NASER ALMADAOJI** (“**ALMADAOJI**”) and there is probable cause to believe that evidence, fruits, and instrumentalities of these violations, as described more

particularly in Attachment B, are present within the information associated with the SUBJECT ACCOUNTS.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause and does not set forth all of my knowledge about this matter.

JURISDICTION

5. This court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PERTINENT FEDERAL STATUTES AND DESIGNATIONS

6. Title 18, United States Code, Section 2339B, prohibits, in pertinent part, a person from knowingly providing “material support or resources to a foreign terrorist organization,” or attempting or conspiring to do the same.

7. The term “material support or resources” means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel..., and transportation, except medicine or religious materials.” 18 U.S.C. Section 2339A(b)(1) and Section 2339B(g)(4). Section 2339B(h) provides that “[n]o person may be prosecuted under this section in connection with the term ‘personnel’ unless that person has knowingly provided, attempted to provide, or conspired to provide a foreign terrorist

organization with 1 or more individuals (who may be or include himself) to work under that terrorist organization's direction or control or to organize, manage, supervise, or otherwise direct that operation of that organization. Individuals who act entirely independent of the foreign terrorist organization to advance its goals or objectives shall not be considered to be working under the foreign terrorist organization's direction and control."

8. On or about October 15, 2004, the United States Secretary of State designated al-Qaeda in Iraq ("AQI"), then known as Jam 'at al Tawid wa' al-Jahid, as a Foreign Terrorist Organization ("FTO") under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive order 13224.

9. On or about May 15, 2014, the Secretary of State amended the designation of AQI as an FTO under Section 219 of the Immigration and Nationality Act and as a Specially Designated Global Terrorist entity under section 1(b) of Executive Order 13224 to add the alias Islamic State of Iraq and the Levant ("ISIL") as its primary name. The Secretary of State also added the following aliases to the FTO listing: The Islamic State of Iraq and al-Sham ("ISIS"—which is how the FTO will be referenced herein), The Islamic State of Iraq and Syria, ad-Dawla al-Islamiyya fi al-Iraq wa-sh-Sham, Daesh, Dawla al Islamiya, and Al-Furquan Establishment for Media Production. On September 21, 2015, the Secretary added the following aliases to the FTO listing: Islamic State, ISIL, and ISIS. To date, ISIS remains a designated FTO.

BACKGROUND INFORMATION

Definitions

10. The following definitions apply to this Affidavit, including all attachments to the Affidavit:

a. **“Internet Service Providers”** or **“ISPs”** are commercial organizations that provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

b. An **“Internet Protocol address”**, also referred to as an **“IP address”**, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client

computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

c. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

d. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

Google Services

11. Google LLC (“Google”) is a multi-national corporation with its headquarters located in Mountain View, California. The company specializes in Internet-related products and services, including an Internet search engine (www.google.com), productivity tools such as email service (gmail), and enterprise products such as Google Search Appliance.

12. Google Photos is a photograph and video sharing and storage service provided by Google, located at photos.google.com. It allows users to back-up their photographs and videos so they can be accessed on any phone, tablet, or computer. It also allows users to pool their photographs and videos together with others into shared albums. Photographs and videos can be organized and searched by places and things in them.

13. Google+ is a social networking and identity service website owned and operated by Google, located at www.plus.google.com. Common features include the following:

- a. Profiles: Users can establish profile pages to maintain personal information, similar to the Facebook and MySpace social networking sites.
- b. Circles: Google+ allows users to establish “circles”, which enables them to organize people into groups for sharing across various Google products and services. This service replaces the typical “Friends” list function used by sites such as Facebook and MySpace.
- c. Communities: Communities allow users with common interests to communicate with each other.
- d. Photos: Google+ allows users to post, back-up, and share photographs. Users can also make comments on photographs posted by other users.
- e. Hangouts: Hangouts are places used to facilitate group video chat. Only Google+ users can join such chats.
- f. Messenger: Messenger is a feature available to Android, iPhone, and SMS devices for communicating through instant messaging within Circles.

14. Google Web and App History is a feature of Google Search in which a user’s search queries and results and activities on other Google services are recorded. The feature is only available for users logged into a Google account. A user’s Web and App History is used to personalize search results with the help of Google Personalized Search and Google Now.

15. Google Play, formerly known as the Android Market, is the official applications store for Android smartphones and tablets. Google makes software applications, music, movies, and books available for purchase and download through the store. Google play allows users of Android devices to purchase, download, and install applications from Google and third-party developers.

16. Location History is a feature on Google accounts that affects all devices. When enabled, Location History allows Google to store a record of all location data from all devices

connected to a Google account.

17. Google Drive is a file storage and synchronization service provided by Google, located at www.drive.google.com. This service provides cloud storage,¹ file sharing, and collaborative editing capabilities. It offers 15 GB of online storage space, which is usable across Google Drive, Gmail, and other Google services.

18. Google Android Backup is a service provided by Google to backup data connected to users' Google accounts. The service allows users to restore data from any Google account that has been backed up in the event that the users' devices are replaced or erased. Data that can be backed up includes Google Calendar settings, WiFi networks and passwords, home screen wallpapers, Gmail settings, applications installed through Google Play, display settings, language and input settings, date and time, and third party application settings and data.

19. YouTube is a video-sharing website owned by Google, located at www.youtube.com. The website allows users to upload, view, and share videos. Most of the content on YouTube has been uploaded by individuals, although media corporations such as CBS and the BBC offer some of their material via the website. Unregistered users can watch the videos, but only registered users can upload videos. Registered users can also post comments about others' uploaded videos.

Email Accounts ("Gmail")

20. Google allows subscribers to obtain e-mail accounts at the domain name gmail.com, like the accounts listed in Attachment A. Subscribers obtain accounts by registering with Google. During the registration process, Google asks subscribers to provide basic personal

¹ Cloud storage is a mechanism in which files can be saved to an off-site storage system maintained by a third party – i.e., files are saved to a remote database instead of the computer's hard drive. The Internet provides the connection between the computer and the database for

information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

21. A Google subscriber can also store with the provider files in addition to e-mails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to e-mails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

22. E-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

23. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and

saving and retrieving the files.

durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

24. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

BACKGROUND OF INVESTIGATION AND PROBABLE CAUSE

25. According to Immigration and Customs Enforcement, **NASER ALMADAOJI** (**ALMADAOJI**) is a 19-year-old individual who was born in Iraq and is a naturalized U.S. citizen. **ALMADAOJI** resides in Beavercreek, Ohio, within the Southern District of Ohio.

FOREIGN TRAVEL AND CBP INTERVIEW

26. Between approximately February 16, 2018, and February 24, 2018, **ALMADAOJI** traveled outside of the United States to the countries of Egypt and Jordan.

27. On or about February 24, 2018, United States Customs and Border Protection (“CBP”) interviewed **ALMADAOJI** upon his re-entry into the United States. **ALMADAOJI** made the following statements during the interview, among others:

- a. **ALMADAOJI** claimed to have traveled by himself and that he traveled to Jordan and Egypt.
- b. **ALMADAOJI** stated that, when in Jordan, he traveled to Irbid, Amman, and to the Israeli border to “see the land that was taken from Jordan.” **ALMADAOJI** claimed he chose to go to Jordan and Cairo, Egypt, because they looked “nice,” but he would not elaborate.
- c. **ALMADAOJI** advised CBP that he had only two friends, and he only talks to two people outside of work, but they are not “religious enough” for him. **ALMADAOJI** advised CBP that he told his family he was going overseas, but he did not tell them when he was coming back to the United States.
- d. **ALMADAOJI** stated he returned to the United States after a taxi driver took off with his backpack and \$3000. He claimed that he reported the incident to the U.S. Embassy.
- e. **ALMADAOJI** advised CBP that at one time he was interested in joining the Marine Corps, but he lost interest because he “became religious” and had “different political views.” **ALMADAOJI** claimed that he had been searching for the “purpose of life” and started focusing on religion. **ALMADAOJI** had come to the conclusion that his purpose was to serve Allah by any means possible.
- f. **ALMADAOJI** referenced U.S. airstrikes that killed Muslims and stated the United States needed to leave the Middle East. **ALMADAOJI** stated he thought about joining the Peshmergan military forces in northern Iraq, but he decided against it. He stated the Peshmergan forces were the “real forces in Iraq to stop ISIS, not U.S.”
- g. **ALMADAOJI**, when asked about his views on ISIS, stated ISIS was “bad for killing other Muslims,” but that most Muslims killed by ISIS were “Shiites.” **ALMADAOJI** stated he is “Sunni” so “Shiites were their natural adversaries.” When asked why he felt like that, he answered “they didn’t follow true Islam” and stated Iraq was a mess right now and the Iraqi government was corrupt and a joke, and that the people of Iraq were no freer now than they were before ISIS invaded Iraq.

28. During the interview, CBP observed approximately four shemagh-style head

wraps in **ALMADAOJI**'s bag. When CBP asked about the shemaghs, **ALMADAOJI** responded he liked the way they looked on "fighters." He was asked if he had seen any fighters while he was in Egypt or Jordan. **ALMADAOJI** stated, "no not really," but that he sees fighters wearing shemaghs online all the time.

SUBJECT GMAIL ACCOUNTS

29. During the February 24, 2018, interview, **ALMADAOJI** provided CBP with his email address—**nasermunshid16@gmail.com**—which is SUBJECT ACCOUNT 1.

ALMADAOJI also provided (937) 969-0509 as his telephone number.

30. On or about May 10, 2018, Google LLC provided a response to a subpoena served on or about May 10, 2018, for SUBJECT ACCOUNT 1. In the response, Google LLC provided subscriber information for SUBJECT ACCOUNT 1, including the name "Abu Ahmad;" phone number (937) 969-0509 as the SMS number associated with the account; and recovery email address of **abubadriralraqi@gmail.com**, which is SUBJECT ACCOUNT 2. The phone number related to SUBJECT ACCOUNT 1 is the same phone number provided by **ALMADAOJI** to CBP. The IP address information provided by Google shows that an individual logged into SUBJECT ACCOUNT 1 from IP addresses resolving to locations in Amman, Jordan; Cairo, Egypt; and Giza, Egypt, between approximately February 16, 2018, and February 22, 2018—the time when **ALMADAOJI** traveled overseas to Jordan and Egypt.

31. On or about June 4, 2018, Google LLC provided a response to a subpoena served on or about May 14, 2018, for SUBJECT ACCOUNT 2. In the response, Google LLC provided subscriber information for SUBJECT ACCOUNT 2, including the name "Abu Muhammad al Iraqi," as well as IP address and log-in information. The IP address information provided by Google shows that SUBJECT ACCOUNT 2 was logged into from IP addresses resolving to

locations in Amman, Jordan; Cairo, Egypt; and Giza, Egypt, between approximately February 16, 2018, and February 22, 2018—the time when **ALMADAOJI** traveled overseas to Jordan and Egypt.

32. On or about June 21, 2018, FBI submitted a letter to Google, requesting that Google preserve information related to the SUBJECT ACCOUNTS for a period of 90-days.

33. On or about June 18, 2018, PayPal identified four accounts under the name **ALMADAOJI**. Three of those accounts listed (937) 969-0509 as the contact number—that is, the same number **ALMADAOJI** identified as his contact number when talking with CBP and the same number associated with email accounts purportedly relating to **ALMADAOJI**. PayPal also identified the same address as that listed for **ALMADAOJI** in the records of the Ohio Bureau of Motor Vehicles (“BMV”).

MESSAGING APPLICATION COMMUNICATIONS

34. Open-source research revealed that **ALMADAOJI**’s phone number, (937) 969-0509, was registered to a publically-available encrypted messaging application with a specific and unique user-identity number. The unique user-identity number was associated with the username @AbuMuhammad16, with a display name (in Arabic) of “Abu Muhammad al-Iraqi.” “Abu Muhammad al Iraqi” is the same general name connected to SUBJECT ACCOUNT 2, as discussed in paragraph 31 above.

35. Based on reporting from a confidential human source (“CHS”), the user name @AbuMuhammad16 was changed to @AbuMuhammad19 in or around July 2018. The unique user-identity number for @AbuMuhammad19 was confirmed to be the same unique number as that specified for @AbuMuhammad16.

36. Between on or about August 5, 2018, and on or about August 19, 2018, an

individual using the encrypted messaging account @AbuMuhammad19, believed to be **ALMADAOJI**, based on the above information, exchanged messages with an undercover employee (“UCE”). The UCE and the individual communicating through the username @AbuMuhammad19 discussed using encrypted messaging applications and other social-media platforms. When the individual was asked by the UCE if the individual knew of other trusted and secured sites to read “dawla news,” the individual replied that he/she was not aware of sites besides “nashir news.”²

37. On August 19, 2018, in a group chat room, the UCE and the individual using the @AbuMuhammad19, along with two other users, exchanged messages regarding the use of thermal imaging on borders and possible ways to avoid detection from thermal-imaging devices. In a one-on-one chat the same day, the individual offered to help the UCE after the UCE explained that he/she was attempting to help a friend cross the border out of Sham³ and into Turkey. The UCE explained that his/her friend lacks monetary resources. The individual using the account associated with **ALMADAOJI** offered to ask around, noting that Sham is a “difficult place and contacts are weak at the moment.” The individual also cautioned that “leaving sham to go back home is seen as treason in most cases and I don’t know how the brothers are gonna take it if i tell them that.”

² Based on my training and experience, and information from other agents, I know the term “dawla” (or “dawlāh”) refers to the Islamic State. I also know that the Nashir News Agency is a propaganda outlet for ISIS.

³ Based on my training and experience, and information from other agents, I know that “Sham” refers to the Levant, a geographic area comprised of Syria, Lebanon, Palestine, and Jordan. I also know that it is commonly used as short-hand to refer to the portions of Syria where ISIS is known to operate.

38. On or about August 15, 2018, the individual using the encrypted messaging account @AbuMuhammad19 communicated in English with an FBI confidential human source who was posing as a France-based contact (hereinafter referred to as Contact #1). During the conversation, the individual informed Contact #1 that he was from Iraq and previously lived in Southern Iraq “with majority shia pigs” before leaving in 2006. The individual stated that the Shia were “everywhere, they’re kicking Ahul al Sunnah from their homes in North Baghdad, Diyala, Salah al Din and other places so they take their homes and spread their filth all over Iraq.” In response to a video that Contact #1 posted during the conversation, which depicted ISIS combat operations in Syria, the individual stated “Alhamdulillah.”

39. On August 16, 2018, the individual using the @AbuMuhammad19 account informed Contact #1 that he recently finished high school, was looking for a job, and was not interested in attending university since he was “not planning to stay in this land much longer.” Contact #1 asked the individual if he was referring to a path for hijra⁴ and the individual responded, “Yes, akhi but I make dua and take every heed there is and Allah Subhanahu wa Ta’ala will find a way for His sincere servants.” Contact #1 offered to put the individual in contact with, who the individual believed to be, a British brother in Iraq who “has helped an old friend of me get to khurassan.”⁵ In response, the individual stated “anything you have is great.”

40. On August 16, 2018, the individual using the encrypted messaging account @AbuMuhammad19, believed to be **ALMADAOJI**, engaged in conversation with the same FBI

⁴ Based on my training and experience, and information from other agents, I know that “Hijra” or “Hijrah” is a term that originally referred to Muhammad’s movement from Mecca to Medina. I also know that the term “hijrah” more recently has been used to refer to traveling from the West to ISIS territory.

⁵ Based on my training and experience, and information from other agents, I know that “khurassan” is a term used to refer to ISIS affiliates in Afghanistan.

confidential human source (that is, the source serving as Contact #1), but the source was now posing as a totally separate person—that being the Iraq-based British contact referenced above in paragraph 39 (hereinafter referred to as Contact #2). During the conversation, the individual using the encrypted messaging application told Contact #2 that he recently met Contact #1 on the messaging application and discussed hijra. At Contact #2’s suggestion, Contact #2 and the individual believed to be **ALMADAOJI** moved the conversation to a secret chat. During the secret chat, the individual believed to be **ALMADAOJI** told Contact #2 that he was not yet ready for hijra, but he was trying to assist a brother in Egypt who was being forced into the Egyptian military in approximately one month. The individual believed to be **ALMADAOJI** stated “I know wilayat Sinai⁶ is not possible at the moment” and inquired “is there a way to Libya or anywhere near egypt.”

41. When Contact #2 inquired why the individual believed to be **ALMADAOJI** was not yet ready for hijra, the individual stated “Right now my problem is money.” The individual believed to be **ALMADAOJI** also told Contact #2 that he was currently in the United States and that he keeps “a low profile.” The individual believed to be **ALMADAOJI** stated: “I want sham but that’s not possible currently but maybe a few months from now when I’m ready.” When asked by Contact #2 who he supported, or who he was trying to join, the individual believed to be **ALMADAOJI** demonstrated operational security by refusing to say exactly who he intended to support when traveling overseas. Rather, the individual stated, “Lol who goes by wilayat” and

⁶ Based on my training and experience, and information from other agents, I know that “Wilayat” translates to “State.” In context, **ALMADAOJI**’s use of the phrase “Wilayat Sinai” refers to ISIS affiliates located in the Sinai Peninsula. The Department of States lists “Wilyat Sinai” as an “aka” of Ansar Bayt al-Maqdis (“ABM”), or ISIL Sinai Province (“ISIL-SP”). ABM was designated as a Foreign Terrorist Organization originally on April 9, 2014. According to the Department of State, in November 2014, ABM officially declared allegiance to ISIL. In September 2015, the Department of State amended ABM’s designation to add the primary name

“I just don’t like to formally say it just in case the authorities here get their hands on these conversations.” When Contact #2 told him that Contact #2 has “spoken to brothers who think I’m AQ” (referring to Al-Qaeda), the individual believed to be **ALMADAOJI** responded “Lol no not those guys.” Contact #2 asked the individual believed to be **ALMADAOJI** why he wanted to make hijra and suggested that “[m]any brothers will say that you are in the best place for jihad.” The individual responded by saying “I don’t like where this is going . . . we’ll stick to hijrah for now.” After Contact #2 stated “I am not trying to push you towards anything I have no way of helping you with something in your own country,” the individual believed to be **ALMADAOJI** stated: “I know this akhi but once there us [sic] hijra then there will jihad in the land of hijra. I don’t like to keep traces back to me that’s why I’m not saying somethings by name just incase I end up messaging the wrong person without knowing.”

42. Between approximately August 18, 2018, and approximately August 20, 2018, the individual believed to be **ALMADAOJI** continued to message with Contact #2. During conversation on August 19, 2018, Contact #2 offered to connect the individual believed to be **ALMADAOJI** with “American brothers who have gone back” and who “often help brothers out.” The individual responded, “That’ll be great akhi ask around and let me know” and “Tell them north east us.” When the individual believed to be **ALMADAOJI** inquired “why did they go back exactly,” Contact #2 stated “Can’t say...your only allowed to leave if the emir has something for you to do. Let’s say that they have projects wherever they are.” The individual believed to be **ALMADAOJI** responded, “Oh I see. I didn’t mean to ask it that way.” Contact #2 stated, “If any of these brothers do get in contact do not mention dawla. What they are doing

has a lot of risk.” The individual believed to be **ALMADAOJI** stated: “No akhi I am well aware of what’s going on, that’s why I’m not mentioning anything by name here.”

43. On or about August 20, 2018, the individual believed to be **ALMADAOJI** discussed his Egyptian associate that was slated to be drafted into the Egyptian military in approximately two months. The individual told Contact #2 that he had “been to egypt once and met” the Egyptian associate there. He stated: “I don’t wanna say here why I was in egypt but him and I planned something and it didn’t work at [sic] well.” Contact # 2 inquired, “Ahh how you know wilaya Sinai is hard to reach?” The individual believed to be **ALMADAOJI** replied “Yea unfortunately I had to learn the hard way despite the fact I was talking to a brother and he told me that himself.” When asked by Contact #2 if the brother had tricked him, the individual believed to be **ALMADAOJI** stated, “No akhi the brother warned me it was difficult to reach Sinai, I don’t know if he was in the lands of Dawlah or just a munasir but no I didn’t end up in prison either.” The individual also stated that no one knows that he was in Egypt, but his family knows he was in Jordan since he was attempting to reach “dar’a”⁷ a second time. Contact #2 asked for the individual’s thoughts on “assisting with some projects in your own country.” After Contact #2 clarified that he/she was talking about the United States, the individual believed to be **ALMADAOJI** stated it was a “big ask,” and asked Contact #2 to “shed a little light on the type of projects.” Contact #2 replied: “It is a big ask, you are not the kind of brother we would ask to take a knife to the street if you know what I mean. There are more important projects there that require intelligent brothers who are determined. I ask only if you would be willing or interested

⁷ Dar’a, also known as Daraa, is a city in southern Syria, located approximately 18 miles east of Irbid, Jordan.

to contribute if hijra is not possible.” The individual believed to be **ALMADAOJI** replied: “Of course I’m always willing.”

44. On or about August 22, 2018, the individual believed to be **ALMADAOJI** continued to communicate in English with Contact #2. The individual turned the conversation toward the topic of United States politics and asked if Contact #2 stayed updated on the subject. Contact #2 told the individual, “I told some of the brothers here about you, they were very impressed and want you to send a bayyah,⁸ two of our local leaders agreed to send you a video to [sic].” The individual believed to be **ALMADAOJI** stated: “In shaa Allah we will then proceed forward with it” and then stated: “But since our talk about projects in the west I did a lot of thinking and I imagined a scenario of the collapse of the US as a nation. They have a lot of weak spots 2 really weak spots that would ignite the deadliest civil war on earth if the right spots are poked.” The individual believed to be **ALMADAOJI** stated the weak spots were “racial issues” and “militias.” When Contact #2 asked if he was talking about starting a race war to destabilize the U.S., the individual believed to be **ALMADAOJI** replied, “Now let’s talk theory and scenario” and proposed the following scenario:

Say someone wanted to convince the militias to start a war with the government They would need proof that the government is planning to end the militia movement which is a US citizen right by the constitution They could do that behind doors. Such as assassinating militia leaders and then blaming it on the government Or hacking into their devices, filling it with child sexual abuse videos, then tipping the fbi abd [sic] the militia leaders get thrown behind bar with atleast 20 years

45. The individual believed to be **ALMADAOJI** then stated that “federal buildings” were “more sensitive for the militias to hit than police stations and military bases.” The

⁸ Based on my training and experience, and information from other agents, I know that bayyah, bayyat, and bayat, are Arabic terms that mean pledge, or oath, of allegiance to a leader.

individual stated, “With a coordinated attack such as car bombings parked next to fed buildings with all the previous build we talked about. And there you have the US on its knees.” The individual believed to be **ALMADAOJI** stated, “It may take a long time to pull something off but it’s long term. This will divide the nation as a whole, including government, military and law enforcement.” The individual told Contact #2, “If you were to mention this to anyone keep it close guarded circle.”

46. On or about August 24, 2018, the individual believed to be **ALMADAOJI** also stated to Contact #2: “After thinking about it for sometime, these projects need secrecy, and lots of it. So there can’t be any physical evidence that leads it back to the I.S.”

47. On August 24, 2018, the FBI confidential source sent a video to the individual believed to be **ALMADAOJI** on the encrypted messaging application. Prior to sending the video, Contact #2 told the individual that “these two brothers have very important positions with us and there [sic] identity and voices must be protected and not shared.” The individual believed to be **ALMADAOJI** then asked Contact #2, “So you told them about the whole plan or part of it?”

48. In the video, Contact #2 and another individual are representing themselves as Iraqi-based ISIS members. The individuals are wearing shemaghs and, what appears to be, both a rifle and knife are visible. In the video, the following, among other things, was stated in Arabic⁹ to the individual believed to be **ALMADAOJI**:

*I am your brother from the State of Islam, Wilayah Iraq, Abu Adhal al Tikreeti, with me here Abu Omar al Faransi who will accept your pledge bayyah to emir almoumeneen.*¹⁰

⁹ Any summaries of, or quotes from, Arabic communications referenced herein are based on preliminary translations.

¹⁰ Emir almoumeneen translates to “Caliph of the Faithful” and, based on training and

In response to receiving the video, the individual believed to be **ALMADAOJI** stated: “A video has never made me smile with sincerity in a while. Give them glad tidings of bay’a tomorrow in shaa Allah.” The individual believed to be **ALMADAOJI** then asked Contact #2 to “destroy [sic] the chat now. The one with the video” and suggested that Contact #2 “might wanna delete the video from your side.”

49. On August 25, 2018, the individual believed to be **ALMADAOJI** communicated with Contact #2, stating “Although I did not get the project done. In shaa Allah expect a video coming soon today.” The individual confirmed with Contact #2 whether he should send the video by way of the encrypted messaging application, stating “Let me know as soon as possible akhi, I’m about to go shoot the video soon.” Contact #2 confirmed that the messaging application was “fine for the video.” The individual believed to be **ALMADAOJI** then told Contact #2 that it would be tomorrow before he would send the video.

50. On or about August 26, 2018, the individual believed to be **ALMADAOJI** told Contact #2 that “Earlier when I tried to go do the video, I felt a sudden need for sleep, I had to force myself up to pray dhur and then went to sleep immediately after. There will be a spiritual struggle to get through with this akhi, I hope you understand if I take a little bit too long to get the video.” Contact #2 replied: “Ok brother send when you can, today or tomorrow will be fine. Fighting here is starting to pick up so I want to make sure we get you in contact with the brothers soon that is my only concern. May Allah guide and facilitate you akhy.” Later that day, the individual forwarded a video to Contact #2 via a separate secret chat session on the messaging application. In the video, a person believed to be **ALMADAOJI** is wearing a scarf that is wrapped in a manner that covers the person’s head and

experience, and information from other agents, I know to be a title that refers to Abu Bakr al-Baghdadi, the self-proclaimed claimed leader of ISIS.

lower face. Under the scarf, a black “beanie” style cap can be seen on the person’s head. The person states the following in Arabic:

Praise be to God and peace and prayers be upon His messenger. I pledge allegiance to Sheikh Abu Bakr al-Baghdadi, the Caliph of the faithful, to obey his command in all situations, in difficulty and in prosperity, and not to dispute orders until I see a common disbelief of which I have a proof from God. God is the witness to what I am saying.

51. During surveillance conducted between on or about May 14, 2018, and on or about September 7, 2018, FBI surveillance observed, on several occasions, **ALMADAOJI** wearing a black knit or “beanie” style cap consistent with the cap worn by the person depicted in the video.

52. On or about August 27, 2018, the individual believed to be **ALMADAOJI** told Contact #2 via the encrypted messaging application that he would not be able to travel to meet brothers currently in the United States and hoped they could pick him up. The individual told Contact #2 that the individual was located in Ohio.

53. Based on my training and experience, I am aware that individuals involved in attempting to provide, or providing, material support and resources to foreign-terrorist organizations often communicate with others involved in similar conduct via e-mail, social-media accounts such as Google+, and online chat programs. I also know based on my training and experience that individuals associated with such activities use YouTube to watch videos and images relating to ISIS and other foreign-terrorist organizations. Those individuals obtain and share such videos and images with each other via a variety of means, including email, social-media accounts, and online-chat programs. Based on my training and experience, I know that individuals involved in material-support offenses often use multiple accounts, aliases, and means to communicate. These multiple accounts or aliases are used as a means to avoid detection from law enforcement.

54. Based on my training and experience, I know that many social media accounts and Internet websites require users to provide their email account when registering for the accounts. The social media account providers and Internet providers then send the users various notifications regarding messages from other users, information accessed by users, information available by the websites, and other information. These messages can provide evidence in cases involving material support offenses because they help in identifying what social media and Internet accounts were utilized by the subjects to communicate with other subjects. In addition, the messages help in identifying the identities of other subjects.

55. Also, as noted above, email providers maintain various subscriber and user information that its users provide when registering for its accounts. Some email providers also require payment for certain services or features. Such information is materially important in cases where online accounts are utilized in connection with attempting to provide or providing material support to a foreign terrorist organization, as this information can help in confirming the identity of the individuals using the accounts and committing the offenses. Email providers maintain various logs of IP addresses utilized to access the accounts. The IP information is again materially important in material support investigations. This information helps in identifying the subjects and the locations where their computer devices are located.

56. Google has the ability to maintain information associated with the web and application history of its users and the location history of its users. Such information is materially relevant in material support investigations, as it may help in identifying websites and applications used or accessed by subjects in relation to the offense, as well as locations involved in the offense.

57. Google Android Backup provides users with the ability to backup data on their

cellular telephones and other electronic devices. Such data can be materially relevant in cases in which cellular telephones and other electronic devices are used to commit or in connection with material support offenses, as this data may provide historical records of their criminal activities that are no longer saved on the devices.

58. As detailed above, **ALMADAOJI** has used a messaging application to discuss matters related to ISIS, potential prospective terrorist activity, and sent a video purporting to pledge allegiance to the self-proclaimed leader of ISIS. Moreover, during communications with Contact #2 on the messaging application, **ALMADAOJI** characterizes his prior travel to Jordan and Egypt as a failed attempt to reach “Wilayat Sinai,” and information from Google indicates that **ALMADAOJI** logged into the SUBJECT ACCOUNTS while in Egypt and Jordan. Based on the foregoing information in this affidavit, I submit there is probable cause to believe that violations of 18 U.S.C. § 2339B have been committed by **ALMADAOJI**, and that evidence, fruits, and instrumentalities of these violations are present within the information associated with the SUBJECT ACCOUNTS.

ELECTRONIC COMMUNICATIONS PRIVACY ACT


59. I anticipate executing the requested warrant for the listed account under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrants to require Google LLC to disclose to the government copies of the records and other information (including the contents of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION


60. Based on my training and experience, and the facts as set forth in this affidavit, I submit that there is probable cause to believe that violations of 18 U.S.C. § 2339B (providing and attempting to provide material support and resources to a foreign terrorist organization) have been committed by **ALMADAOJI**, and that there is probable cause to believe that, present within the information associated with the SUBJECT ACCOUNTS, as described more particularly in Attachment A, is evidence, fruits, and instrumentalities of these violations, as described more particularly in Attachment B.

61. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

62. Because the warrant for the account described in Attachment A will be served on Google LLC, who will then compile the requested records at times convenient to that entity, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.


Special Agent P. Andrew Gagan
Federal Bureau of Investigation

SUBSCRIBED and SWORN before me this 21st day of September 2018.


HON. SHARON L. OVINGTON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

This warrant applies to information associated with **nasermunshid16@gmail.com**, and **abubadriliraqi@gmail.com** (collectively, the “SUBJECT ACCOUNTS”), which is stored at premises controlled by Google LLC, a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any e-mails, records, files, logs, or information that has been deleted, but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for the SUBJECT ACCOUNTS:

1. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
3. The types of service used;
4. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;
6. Subscriber registration information;
7. Sign-in IP addresses and associated time stamps;
8. Video upload IP addresses and associated time stamps;
9. Copies of private videos and associated video information, to include any deleted videos;
10. Private message contents and comments, to include any deleted messages or comments;

11. Public message contents and comments, to include any deleted messages or comments;
12. YouTube search history and any information referring or relating to any videos uploaded, viewed, or transmitted, and any comments, or other communication, involving the YouTube platform;
13. Information that refers or relates to subscriber and registration information;
14. Information that refers or relates to internet history, including browser history, and app history, including app data;
15. Information that refers or relates to IP logs associated with the internet history and app history;
16. Google search history;
17. Google browser activity (including activity on Google Chrome);
18. Any available backup data for any electronic devices;
19. Information that refers to Google change history and change information;
20. Cellular device information, including IMEI/MEID, make and model, serial number, date and IP address of last access to Google, and a list of all accounts that have ever been active on the device;
21. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;
22. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored;
23. Any cookies-related information concerning the account;
24. Google Play purchase history and transactional records, including payment method(s) and related billing information;
25. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

26. Location history.

Pursuant to the warrant, Google LLC, shall disclose responsive data by sending it to the Federal Bureau of Investigation, or making the data available to the Federal Bureau of Investigation via Google LLC's, electronic portal, within 14 days of the issuance of this warrant.

II. Information to be seized by the government

1. All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of offenses involving providing, conspiring, or attempting to provide material support and resources to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B, involving the user of the accounts, and occurring from June 1, 2017, to the present, for each account or identifier listed on Attachment A, information referring, relating, or pertaining to the following:

- a. Email, text, and other messages, photos, videos, contacts and contact lists, addresses and address books, voicemail messages, location data, calendar, applications and application data, settings, location data, web-search history, YouTube search history, YouTube comments and communications and messaging, comments and communications and messaging on other platforms, information stored on Google Chrome, and other social-media platforms;
- b. Records and information referring, or relating, to terrorist activity, ISIS, or any other foreign terrorist organizations;
- c. Records and information referring, or relating, to the provision, or attempted provision, of material support or resources to ISIS, or any other foreign terrorist organizations;
- d. Records and information referring, or relating, to travel, including travel plans, itineraries, reservations, bookings, tickets, and the means and sources of payment for travel;
- e. Records and information referring, or relating, to plans to commit a terrorist attack, or to fight with ISIS, or any other foreign terrorist organizations, including, without limitation, funding, materials, maps, disguises, aliases, weapons, or other materials that may assist with an attack;
- f. Records and information referring, or relating, to communications with individuals relating to ISIS, or any other foreign terrorist organizations, or potential terrorist attacks on the United States, including any preparation for such attacks on the United States, or in other countries;
- g. Records and information relating to the use of YouTube, Facebook, WhatsApp, and other forms of social media, use of the internet, and communication methods, including private messaging, where such information refers or relates in anyway to terrorist attacks, ISIS, or any other foreign terrorist organizations;

- h. Records and information referring, or relating, to videos or other content created, publicly posted, or viewed on the internet where such content concerns terrorist activity, ISIS, or any other foreign terrorist organizations;
- i. Communications involving, referring, or relating to potential co-conspirators, accomplices, and associates, concerning terrorist activities, ISIS, or any other foreign terrorist organizations, or relating to providing, or attempting to provide, material support or resources for such organizations;
- j. Identifying information and contact information of potential co-conspirators, accomplices, associates, and other individuals engaged, or otherwise involved, in terrorist activity, providing, or attempting to provide, material support or resources to ISIS, or any other foreign terrorist organizations;
- k. The timing of communications among potential co-conspirators, accomplices, associates, and other individuals engaged, or otherwise involved, in terrorist activity, or providing, or attempting to provide, material support or resources to ISIS, or any other foreign-terrorist organizations;
- l. Information referring, or relating to, the methods and techniques used in terrorist activity, or providing, or attempting to provide, material support or resources to a foreign-terrorist organization;
- m. The distribution of videos and photographs referring, or relating to, the work, accomplishments, or propaganda of terrorists or a foreign-terrorist organization;
- n. Information referring, or relating, to any offer of support and services, including translation services, to a foreign-terrorist organization;
- o. Information referring, or relating to, the recruitment of fighters, supporters, and financial support for a foreign-terrorist organization;
- p. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- q. Records and information indicating the account user's state of mind as it relates to terrorist activity, or the provision, or attempted provision, of material support or resources to ISIS, or other foreign terrorist organizations;
- r. Records of Internet Protocol addresses used;
- s. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

- t. The identity of the person(s) who created, used, or deleted the email account, including information that would help reveal the whereabouts of such person;
 - u. The identity of any person(s) who communicated with the email account about matters relating to terrorist activity, or foreign-terrorist organizations, and any records related to the whereabouts of such persons;
 - v. Records indicating that data has been deleted by the account owner, potentially to hide evidence of a crime; and
 - w. Account history (including Terms of Service and any complaints) and billing records (including date, time, duration, and screen names used each time the accounts were activated).
2. Evidence of user attribution showing who used, or owned, the account at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.
3. As used above, the terms “records” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.